

CLAIMS

What is claimed is:

- 1 1. A method for providing security, the method comprising the steps of:
2 detecting when a request for an action is made by a principal; and
3 determining whether said action is authorized based on an association
4 between permissions and a plurality of routines in a calling hierarchy
5 ~~associated with said principal.~~
- 1 2. The method of Claim 1, wherein:
2 the step of detecting when a request for an action is made includes detecting
3 when a request for an action is made by a thread; and
4 the step of determining whether said action is authorized includes
5 determining whether said action is authorized based on an association
6 between permissions and a plurality of routines in a calling hierarchy
7 associated with said thread.
- 1 3. The method of Claim 1, wherein:
2 the calling hierarchy includes a first routine; and
3 the step of determining whether said action is authorized further includes
4 determining whether a permission required to perform said action is
5 encompassed by at least one permission associated with said first
6 routine.

sub
a²

1 4. The method of Claim 3, wherein said association between permissions and
2 said plurality of routines is based on a first association between protection
3 domains and permissions.

1 5. The method of Claim 4, wherein:
2 each routine of said plurality of routines is associated with a class; and
3 said association between permissions and said plurality of routines is based
4 ~~on a second association between classes and protection domains.~~

1 4. The method of Claim 1, wherein the step of determining whether said action
2 is authorized further includes determining whether a permission required to
3 perform said action is encompassed by at least one permission associated
4 with each routine in said calling hierarchy.

sub
a²

1 7. The method of Claim 1, wherein:
2 a first routine in said calling hierarchy is privileged; and
3 wherein the step of determining whether said action is authorized further
4 includes determining whether a permission required to perform said
5 action is encompassed by at least one permission associated with each
6 routine in said calling hierarchy between and including said first
7 routine and a second routine in said calling hierarchy, wherein said
8 second routine is invoked after said first routine, wherein said second
9 routine is performing said requested action.

1 7. The method of Claim 6, wherein the step of determining whether said
2 permission required to perform said action is encompassed by at least one
3 permission associated with each routine in said calling hierarchy between
4 and including said first routine and said second routine further includes the
5 steps of:
6 determining whether said permission required is encompassed by at least one
7 permission associated with said second routine; and
8 in response to determining said permission required is encompassed by at
9 least one permission associated with said second routine, then
10 performing the steps of:
11 A) selecting a next routine from said plurality of routines in said
12 calling hierarchy,
13 B) if said permission required is not encompassed by at least one
14 permission associated with said next routine, then transmitting
15 a message indicating that said permission required is not
16 authorized, and
17 C) repeating steps A and B until:
18 said permission required is not authorized by at least one
19 permission associated with said next routine,
20 there are no more routines to select from said plurality of
21 routines in said calling hierarchy, or
22 determining that said next routine is said first routine.

1 ⁸/₉. The method of Claim ⁷/₈, wherein:
2 the method further includes the step of setting a flag associated with said first
3 routine to indicate that said first routine is privileged; and
4 the step of determining that said next routine is said first routine includes
5 determining that a flag associated with said next routine indicates said
6 next routine is privileged.

1 ⁹/₁₀. The method of Claim ⁸/₉, wherein the step of setting said flag associated with
2 said first routine includes setting a flag in a frame in said calling hierarchy
3 associated with said thread.

1 11. A computer-readable medium carrying one or more sequences of one or
2 more instructions, wherein the execution of the one or more sequences of the
3 one or more instructions causes the one or more processors to perform the
4 steps of:
5 detecting when a request for an action is made by a principal; and
6 determining whether said action is authorized based on an association
7 between permissions and a plurality of routines in a calling hierarchy
8 ~~associated with said principal.~~

1 ¹¹/₁₂. The computer-readable medium of Claim ¹⁰/₁₁, wherein:
2 the step of detecting when a request for an action is made includes detecting
3 when a request for an action is made by a thread; and

1 ~~12~~ The computer readable medium of Claim ~~11~~¹⁰, wherein:
2 the calling hierarchy includes a first routine; and
3 the step of determining whether said action is authorized further includes
4 determining whether a permission required to perform said action is
5 encompassed by at least one permission associated with said first
6 routine.

1 15. The computer-readable medium of Claim 11, wherein:
2 each routine of said plurality of routines is associated with a class; and
3 said association between permissions and said plurality of routines is based
4 ~~on a second association between classes and protection domains.~~

44

Sub B4
17. The computer readable medium of Claim 11, wherein:
a first routine in said calling hierarchy is privileged; and
wherein the step of determining whether said action is authorized further
includes determining whether a permission required to perform said
action is encompassed by at least one permission associated with each
routine in said calling hierarchy between and including said first
routine and a second routine in said calling hierarchy, wherein said
second routine is invoked after said first routine, wherein said second
routine is performing said requested action.

16
18. The computer readable medium of Claim 15, wherein the step of determining
whether said permission required to perform said action is encompassed by
at least one permission associated with each routine in said calling hierarchy
between and including said first routine and said second routine further
includes the steps of:
determining whether said permission required is encompassed by at least one
permission associated with said second routine; and
in response to determining said permission required is encompassed by at
least one permission associated with said second routine, then
performing the steps of:
A) selecting a next routine from said plurality of routines in said
calling hierarchy,

13 B) if said permission required is not encompassed by at least one
14 permission associated with said next routine, then transmitting
15 a message indicating that said permission required is not
16 authorized, and
17 C) repeating steps A and B until:
18 said permission required is not authorized by at least one
19 permission associated with said next routine,
20 there are no more routines to select from said plurality of
21 routines in said calling hierarchy, or
22 determining that said next routine is said first routine.
23

1 ¹⁷~~19~~. The computer readable medium of Claim ¹⁶~~18~~, wherein:
2 the computer readable medium further comprises one or more instructions
3 for performing the step of setting a flag associated with said first
4 routine to indicate that said first routine is privileged; and
5 the step of determining that said next routine is said first routine includes
6 determining that a flag associated with said next routine indicates said
7 next routine is privileged.

1 ¹⁸~~20~~. The computer readable medium of Claim ¹⁷~~19~~, wherein the step of setting said
2 flag associated with said first routine includes setting a flag in a frame in said
3 calling hierarchy associated with said thread.

1 21. A computer system comprising:

sub
A7

2 a processor;
3 a memory coupled to said processor;
4 said processor being configured to detect when a request for an action is
5 made by a principal; and
6 said processor being configured to determine whether said action is
7 authorized based on an association between permissions and a
8 plurality of routines in a calling hierarchy associated with said
9 principal.

1 22. The computer system of Claim 21, wherein said processor is configured to
2 determine whether said action is authorized by determining whether a
3 permission required to perform said action is encompassed by at least one
4 permission associated with said first routine.

23. The computer system of Claim 21, said processor is configured to determine
whether said action is authorized by determining whether a permission
required to perform said action is encompassed by at least one permission
~~associated with each routine in said calling hierarchy.~~